# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/20074

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/00( 2006.01)**

USPC: 713/175
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/175

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | USPub 2006/0236122 (FIELD et al), October 19, 2006 (10/19/2006), paragraphs 55-57. | 1-8, 18-21 |
| Y | 2006/0153368 A1 (BEESON), July 13 2006 (07/13/2006), paragraphs 21 and 35. | 1-8, 18-21 |
| Y | US 6,751,729 (GINIGER et al) June 15, 2004 (06/15/2004), column 12-column 13 and Fig. 5b. | 1-3, 8 and 21 |
| Y | US 6,278,782 B1 (OBER et al) August 21, 2001 (08/21/2001), column 2 lines 36-40. | 7, 19 |
| Y | | |
| Y | | |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
05 September 2008 (05.09.2008)

Date of mailing of the international search report
08 OCT 2008

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (571) 273-3201

Authorized officer
KAMBIZ ZAND

Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (April 2007)

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/20074

**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:
Please See Continuation Sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of any additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1-8 and 18-21

**Remark on Protest**

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

BOX III. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING

Group 1, claim(s) 1-8 and 18-21, drawn to a device computing a public key as a function of the private key and constructing a device certificate as a function of the device ID,

Group 2, claim(s), 9-14 drawn to a server comprising a number generator generating a first number, a certificate request module generating a request for a device certificate, an interface sending a response that includes a second number, a second signature that is generated with the second number and a device certificate, and a certificate verification module verifying that the first number and the second number match,

Group 3, claim(s), claims 15-17 and 24 drawn to a device initializing a state variable to an initial value, computing a key as a function of a secret seed random number, incrementing the sequence number, generating a random number as a function of a key and the state variable, incrementing the state variable and generating a random number using the key and incremented state variable,

Group 4, claim(s), claims 22-23 drawn to a device comprising a secure processor and a secure on-chip memory including a security kernel having an authenticated security API.

This International Searching Authority considers the international application does not comply with the requirements of unity of invention (Rules 13.1, 13.2 and 13.3) for the reasons indicated below:

The invention listed as Groups 1-5 do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2 they lack the same or corresponding special technical feature for the following reasons: Group 1 relates to computing a public key as a function of the private key and a device certificate as a function of the device ID, Group 2 relates to generating of a first number, a second number, a second signature and a certificate, and verifying that the first number and the second number match, and Group 3 relates to computations involving initializing a state variable, an initial value, and generating a random number and a key, Group 4 relates to security kernel generating a device certificate.